UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/709,657	05/20/2004	David John OTWAY	2006579-0218	3656

24280 7590 06/16/2006

CHOATE, HALL & STEWART LLP
TWO INTERNATIONAL PLACE
BOSTON, MA 02110

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 06/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/709,657	OTWAY ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,9 and 12-23* is/are rejected.

7)☒ Claim(s) *7, 10, and 11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 May 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/18/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 have been examined.

Priority

2. The instant application has been filed as a divisional application of Patent Application No. 09/617,380, now U.S. Patent No. 7,020,773, filed 17 June 2000.

3. The claims presented in the instant application were originally presented as claims 49-72 in the parent application, and were not elected in response to the restriction requirement to that application mailed 4 March 2004.

Information Disclosure Statement

4. The following Information Disclosure Statement in the instant application has been fully considered except as noted below:

IDS filed 18 April 2005.

5. On page 2 of the IDS filed 18 April 2005, a reference is made to application 10/706,117, which appears to be unrelated to the instant application. It is being

presumed that this was meant to refer to 09/706,117, which is commonly assigned with the parent application of the instant application.

6. On page 2 of the IDS filed 18 April 2005, a reference is made to U.S. Patent No. 5,515,111. This publication is not listed in the Form 1449 and has not been considered.

7. Item C11 in the IDS filed 18 April 2005 is illegible and has not been considered.

8. Items B10, B13, C4, C5, C13, C18, C19, and C20 have not been found in the file wrapper of the instant application or of the parent application and have not been considered.

Specification

9. The abstract of the disclosure is objected to because it is not a single paragraph. Correction is required. See MPEP § 608.01(b).

10. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

In claim 7, Applicant recites a communication between the first computer and the verifier, a communication between the verifier and the second computer, and, in base

claim 1, a communication between the first and second computers wherein each communication uses the same channel (i.e. the second communication channel) to send the same message (i.e. the second message). Applicant's specification clearly discloses that different channels are used for each of these communications (see abstract; paragraphs 6-8; and items 15, 40, and 55 in figure 1) and there is nothing in the specification to suggest that these may be a common channel or that one channel can comprise the other two.

Claim Objections

11. Claims 7, 10, and 11 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

In claim 7, the definition of the second communication channel, over which the second message is being sent, appears to encompass more connections (i.e. connections between the first computer and the verifier and between the second computer and the verifier) than just the connection between the first and second computers, as recited in base claim 1. Since this definition broadens the scope of the second communications channel, claim 7 is an improper dependent claim.

Claims 10 and 11 depend from claim 7, and include all the limitations of that claim, thereby rendering those dependent claims improper.

It is unclear, in light of the specification, what Applicant is attempting to claim in claim 7. Claims 7, 10, and 11 shall therefore not be treated further on the merits in this action.

12. Claim 16 is objected to because of the following informalities: In the next to last line, the word "sdaid" is not a word. It is being presumed that this should read "said." Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 5, 12, and 14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 5 and 12 recite the limitation "said first authentication number" in lines 2-3 and 3-4, respectively. There is insufficient antecedent basis for this limitation in these claims. It is being presumed that claims 5 and 12 each depend on claim 2.

Claim 14 recites the limitation "said third message" in line 3. There is insufficient antecedent basis for this limitation in the claim. It is being presumed that claim 14 is dependent on claim 13.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

14. Claims 1-5, 8, 12, 16, 21, and 22 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,745,574 to Muftic.

As per claims 1-3, 12, 21, and 22, Muftic discloses an arrangement wherein a public key certificate, which includes a system's public key (see column 10, lines 37-39) (the second authentication number) has been stored by a Certification Authority (CA) over a communications channel (the second communications channel). A Certificate_Signature_Request message is then sent via a different communications channel ("any other way," see column 11, line 32) by the system to the common repository or CA (i.e. the first communications channel) which includes encrypted material (the first message), such as a signature (a type of authentication number) using the system's private key, which is decryptable using the public key that has previously been sent (see column 11, lines 30-53) to a common repository (see column 7, lines 4-12).

Regarding claim 4, it is inherent that any one of a number of additional parameters must be included to properly send a message such as Certificate_Signature_Request, and any such parameter constitutes a first indicia.

As per claim 5, the signature is derived from values stored on the first computer, so it must be generated on the first computer; the first computer's public key also is generated there if the first computer is a CA (see column 10, lines 11-18).

Regarding claim 8, a communication channel inherently comprises a communication channel.

Regarding claim 16, the first transmitter is the system and the first receiver is the repository.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 6, 9, 13-15, 17-20, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,745,574 to Muftic.

Regarding claims 6 and 9, Muftic does not disclose the further use of encryption in the public key certificate sending transaction.

Muftic, however, further discusses the use of cryptography in the prior art discussion, noting that material encrypted with a public key may be decrypted with the corresponding private key, and vice-versa, and that a message may be authenticated by encryption data with a key known only to authorized persons, to tell the recipient that a message came from an authorized source (see column 1, lines 34-56). Muftic further discloses the using of a session key, which is exchanged by encrypting it using public key cryptography, for encrypting the remainder of the transaction or session, so that the encryption and decryption times are quicker (see column 2, lines 47-52).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify Muftic's invention by using a session key for the remainder of the certificate sending transaction and use message authentication, as is disclosed by Muftic's prior art, to tell the recipient that a message came from an authorized source with quicker encryption and decryption times.

The establishment and use of a session key in Muftic invention would result in the inclusion of the encrypted session key in the first message of the transaction (the second message). In this case, the encrypted session key, generated at the system, is the "first authentication number" and the digital signature is the "third authentication number" (rather than being the "first authentication number" as per the rejections under 35 U.S.C. 102).

Regarding claims 13, 14, 17, and 23 the second computer replies to Muftic's Certificate_Signature_Request with a Certificate_Signature_Reply (the third message) that includes the decrypted certificate (which comprises the public key) of the first

computer. Since all messages in the session are being encrypted with the session key, this results in the second authentication number being encrypted by the first authentication number, which is then decrypted for authentication.

Regarding claims 15, 19, and 20, though Muftic does not disclose the encrypting of the original distribution of the public key, one skilled in the art would likewise modify the invention of Muftic by adding encrypted authentication material to the initial distribution of the public key, as disclosed in the prior art, to tell the recipient that a message came from an authorized source (confirmed by the recipient by using a verifier).

Regarding claim 18, the authentication of messages disclosed by Muftic requires a comparator to determine whether the values match.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques, can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

June 9, 2006

Matthew Heneghan, USPTO Art Unit 2134